Amendment to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing, **by the first digital certificate issuing authority,** the electronic document to obtain a once signed electronic document; ~~**and**~~

transmitting the once signed electronic document to a second digital certificate issuing authority ~~**to obtain a twice signed electronic document; and**~~

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document,

wherein the second digital issuing authority is hierarchically superior to the first digital certificate issuing authority.

2. (Currently Amended) The method of claim 1 wherein signing the electronic document to obtain a once signed electronic document **further** comprises:

~~**obtaining a hash value using contents of the electronic document**~~ **providing,** as input to a hash algorithm, **the contents of the electronic document**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

~~storing~~ **writing** the encrypted hash value in the electronic document.

3. (Currently Amended) The method of claim 1 wherein ~~obtaining~~ **signing, by the second digital certificate issuing authority, the once signed electronic document to obtain** a twice signed electronic document **further** comprises**:** ~~at least one of~~

writing the second digital certificate issuing ~~authority inserting its~~ **authority's** authenticating information in the once signed electronic document**[[,]] ;**

~~obtaining a hash value using contents of the electronic document~~ **providing,** as input to a hash algorithm, **the contents of the electronic document;**

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key**[[,]] ; and**

~~including~~ **writing** the encrypted hash value in the electronic document~~, and~~

~~transmitting the twice signed electronic document~~.

4. (Currently Amended) The method of claim 3 wherein ~~obtaining a~~ **calculating the** hash value ~~using contents of the electronic document as input to a hash algorithm~~ comprises ~~at least one of, using~~ **providing as input to the hash algorithm at least one of:**

the party's authenticating information~~, using~~ **;**

the first digital certificate issuing authority's authenticating information~~, using~~ **;**

the digital signature of the first digital certificate issuing authority[[,]] ; and ~~using~~ the second digital certificate issuing authority's authenticating information ~~as input to a hash algorithm~~.

5. (Original) The method of claim 1, wherein writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

6. (Currently amended) A ~~computer~~ system comprising:

a bus;

a1

a data storage device coupled to said bus; and

a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing, **by the first digital certificate issuing authority,** the electronic document to obtain a once signed electronic document; ~~and~~

transmitting the once signed electronic document to a second digital certificate issuing authority; **and**

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document,

wherein the second digital issuing authority is hierarchically superior to the first digital certificate issuing authority.

7. (Currently amended) A ~~computer~~ system as in claim 6 wherein signing the electronic document to obtain a once signed electronic document comprises:

~~obtaining a hash value using contents of the electronic document~~ **providing,** as input to a hash algorithm**, the contents of the electronic document**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

~~storing~~ **writing** the encrypted hash value in the electronic document.

8. (Currently amended) A ~~computer~~ system as in claim 6 wherein ~~obtaining~~ **signing, by the second digital certificate issuing authority, the once signed electronic document to obtain** a twice signed electronic document comprises**:** ~~at least one of~~

writing the second digital certificate issuing ~~authority inserting its~~ **authority's** authenticating information in the once signed electronic document**[[,]] ;**

~~obtaining a hash value using contents of the electronic document~~ **providing,** as input to a hash algorithm, **the contents of the electronic document;**

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key**[[,]] ; and**

~~including~~ **writing** the encrypted hash value in the electronic document~~, and~~

~~transmitting the twice signed electronic document~~.

9. (Currently amended) A ~~computer~~ system as in claim 8 wherein ~~obtaining a~~ **calculating the** hash value ~~using contents of the electronic document as input to a hash algorithm~~ comprises ~~at least one of, using~~ **providing as input to the hash algorithm at least one of:**

the party's authenticating information~~, using~~ **;**

the first digital certificate issuing authority's authenticating information~~, using~~ **;**

the digital signature of the first digital certificate issuing authority[[,]] **;** and ~~using~~

the second digital certificate issuing authority's authenticating information ~~as input to a hash algorithm~~.

10. (Currently amended) A ~~computer~~ system as in claim 6 wherein writing a party's authenticating information and a first digital certificate issuing ~~authorities~~ **authority's** authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

11. (Currently amended) An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising**:**

writing a party's authenticating information and a first digital certificate issuing ~~authorities~~ **authority's** authenticating information in an electronic document;

signing, **by the first digital certificate issuing authority,** the electronic document to obtain a once signed electronic document; ~~and~~

transmitting the once signed electronic document to a second digital certificate issuing authority ~~to obtain a twice signed electronic document~~ **; and**

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document,

wherein the second digital issuing authority is hierarchically superior to the first digital certificate issuing.

12. (Currently amended) An article of manufacture as in claim 11 wherein signing the electronic document to obtain a once signed electronic document **further** comprises:

~~obtaining a hash value using contents of the electronic document~~ **providing,** as input to a hash algorithm**, the contents of the electronic document**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

~~storing~~ **writing** the encrypted hash value in the electronic document.

13. (Currently amended) An article of manufacture as in claim 11 wherein ~~obtaining~~ **signing, by the second digital certificate issuing authority, the once signed electronic document to obtain** a twice signed electronic document **further** comprises**:** ~~at least one of~~

writing the second digital certificate issuing ~~authority inserting its~~ **authority's** authenticating information in the once signed electronic document**[[,]] ;**

~~obtaining a hash value using contents of the electronic document~~ **providing,** as input to a hash algorithm, **the contents of the electronic document;**

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key**[[,]] ; and**

~~including~~ **writing** the encrypted hash value in the electronic document~~, and transmitting the twice signed electronic document~~.

14. (Currently amended) An article of manufacture as in claim 13 wherein ~~obtaining a~~ **calculating the** hash value ~~using contents of the electronic document as input to a hash algorithm~~ comprises ~~at least one of, using~~ **providing as input to the hash algorithm at least one of:**

the party's authenticating information~~, using~~ **;**

the first digital certificate issuing authorities authenticating information~~, using~~ **;**

the digital signature of the first digital certificate issuing authority**[[,]] ;** and ~~using~~

the second digital certificate issuing authority's authenticating information ~~as input to a hash algorithm~~.

15. (Original) An article of manufacture as in claim 11 wherein writing a party's authenticating information and a first digital certificate issuing authorities authenticating

information in an electronic document comprises receiving the party's authenticating information via a secure connection.

16. (Currently amended) A method comprising:

receiving**, from a first digital certificate issuing authority,** a once signed electronic document **at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority**;

writing **[[a]] the second** digital certificate issuing authority's authenticating information in the once signed electronic document; **and**

signing**, by the second digital certificate authority,** the once signed electronic document to form a twice signed electronic document**~~; and~~**

~~transmitting the twice signed electronic document~~.

17. (Currently Amended) The method of claim 16 wherein signing**, by the second digital certificate authority,** the once signed electronic document to form a twice signed electronic document **further** comprises:

~~obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information~~ providing, as input to a hash algorithm**, the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the **second** digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

18. (Currently amended) A ~~computer~~ system comprising:

a bus;

a data storage device coupled to said bus; and

a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

receiving, **from a first digital certificate issuing authority,** a once signed electronic document **at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority**;

writing **[[a]] the second** digital certificate issuing authority's authenticating information in the once signed electronic document;

signing, **by the second digital certificate issuing authority,** the once signed electronic document to form a twice signed electronic document~~; and~~

~~transmitting the twice signed electronic document~~.

19. (Currently Amended) A ~~computer~~ system as in claim 18 wherein signing, **by the second digital certificate issuing authority,** the once signed electronic document to form a twice signed electronic document **further** comprises:

~~obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information~~ **providing,** as input to a hash algorithm**, the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the **second** digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

20. (Currently Amended) An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising**:**

receiving**, from a first digital certificate issuing authority,** a once signed electronic document **at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority**;

writing **[[a]] the second** digital certificate issuing authority's authenticating information in the once signed electronic document;

signing**, by the second digital certificate issuing authority,** the once signed electronic document to form a twice signed electronic document~~; and~~

~~transmitting the twice signed electronic document~~.

21. (Currently amended) An article of manufacture as in claim 20 wherein signing, **by the second digital certificate issuing authority,** the once signed electronic document to form a twice signed electronic document **further** comprises:

~~**obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information**~~ **providing,** as input to a hash algorithm, **the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information**;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the **second** digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

22. (New) The method of claim 1 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

23. (New) The computer system of claim 6 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

24. (New) The article of manufacture of claim 11 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

25. (New) The method of claim 16 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

26. (New) The computer system of claim 18 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

A1

27. (New) The article of manufacture of claim 20 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.